EC-2000-007
IV-D-122

Larry Bunting
TN Division of Water Pollution Control
401 Church Street, 6th Floor Annex
Nashville TN 37243

United States Environmental Protection Agency
Enforcement and Compliance Docket and Information Center
Mail Code 2201A
Attn: Docket Number EC-2000-007
1200 Pennsylvania Avenue NW
Washington DC 20460

Re: Comment on Establishment of Electronic Reporting: Electronic Records; Proposed Rule proposed in Federal Register August 31, 2001 (66 FR 46162)

I thank EPA for the opportunity to comment and for allowing time extensions for comments on the rule proposal for Cross Media Electronic Reporting and Recordkeeping. Electronic recordkeeping and reporting systems used in the future will be vital to both the permittees and regulators. All the issues need to be addressed at this time. EPA should address issues that restrict electronic submittals such as requirements for "certified mail," "written request," etc. Terms in regulations written before the advent of extensive electronic communication should be revised to show electronic communication is acceptable. At the same time, the intent of the regulations for adequate documentation needs to be kept, regardless of changes in wording to rules. This is now technologically feasible for electronic submissions.

Much of the rule proposal seem focused on transmittal of information to EPA. There will be time for regulated entities to adapt to whatever criteria EPA promulgates. In this area, EPA needs to understand that current efforts have been taken by some states and regulated entities that must be adapted to whatever EPA promulgates. The adaptation may have some costs. Not knowing the details of how the approvals will be handled leaves much uncertainty over the cost of the effort. It does allow for freedom and some flexibility, but also raises fear that poor communication can lead to defeat of the program strategy.

The recordkeeping portion of the proposal may be more of a problem in this proposal. States and regulated entities that already have set up electronic recordkeeping will have less flexibility adapting to EPA's recordkeeping requirements. Even where environmental recordkeeping is not yet active, the use of electronic records in other, non-environmental existing systems may ultimately mean those systems will have to be changed to conform to EPA's criteria. The proposed rule may be more far-reaching than EPA thinks. Regulation of recordkeeping systems is a large and expensive undertaking for all parties and EPA should not oversimplify the situation.

1. What constitutes a "record"?

The proposal seems to allow an all-encompassing view of what constitutes a

record. In a paper system, people exercise control over what is to be saved as a "record," and not everything is saved for pragmatic reasons. The pervasive extent that could apply to electronic recordkeeping may represent a substantial expansion of recordkeeping beyond what is now tracked in a paper system. EPA indicates that the electronic system should be as good as the paper system but also states that it wants to improve the recordkeeping. There is a mixed signal here and much ambivalence about what "records" EPA is thinking of for which "recordkeeping" would apply. Paper records and electronic records are quite different in some respects. Electronic systems can handle, store and give access to much more information than could be handled in a paper system. Access is quicker, searches more easy. The form of the storage in electronic records can include video, audio, and materials not amenable to storage on paper, as well as more comprehensive storage of records that do exist on paper formats.

If the recordkeeping is to become more extensive and go beyond the level of paper systems, there are a number of questions that must be answered. There is no mention of how privacy issues will be addressed in recordkeeping systems to protect personal information. There are no examples of what must be considered a record. For instance, is raw electronic data from a temperature probe to be treated as a "record," or will the interpreted data be the "record," or both? Does laboratory data originating and maintained in a third party laboratory computer system become part of the "record" that must be stored? Stored in whose system? Will drafts of a report written up on a word processor become successive "records" that must be kept? Do all email correspondences gain status as "record" if permit-related issues are in it? If stringently interpreted, almost anything maintained or originated in electronic format is going to be subject to electronic recordkeeping and EPA is going to have the regulatory "say-so" on its storage and preservation. EPA needs to provide better guidance on what is specifically intended by the term "record" so that extent and costs of the rule can be better estimated.

There are additional problems on 'records' that should be addressed. Electronic data storage abilities will allow a possibility for regulators to use data mining techniques to uncover deliberate falsification of data. What are the limits to these "searches" and what is the extent to which regulators can pursue information within another's computer system? Raw data can be seriously flawed and easily misinterpreted. Data mining techniques have drawbacks where raw information is misinterpreted. If recordkeeping is going to be pushed back to the point of keeping raw data, how will EPA address these limitations? The rule mentions legitimate concerns about data falsification, permittees have legitimate concerns about misinterpretation of dubious data mined out of an electronic recordkeeping system where such records have been required to be kept by those regulators. If regulators request information and the results are questionable to a permittee, what mechanism will be in place to allow analysis of data prior to, or after, submittal of a report to an agency? Rather than creating a system where all raw information becomes a record, self-reporting entities should be left to perform the function of collecting appropriate documentation to support the submittal claims and storing it securely. Support for the claims is the business of the manager making certification who should have some flexibility in determining what constitutes the record. Regulators need a mechanism to give feedback on the quality of the supporting record storage.

2. Current data storage in electronic formats

Criteria for electronic recordkeeping systems needs to consider current data stored in electronic formats, the size of the entities involved and relative costs and risks for data storage and record storage. Existing information on computers, backup and support which will have to be transformed into an electronically secure recordkeeping system with attendant "chain-of-custody" requirements. This is a big step. Many with electronic records do not have an option of returning to systems based entirely on paper. In many cases monthly reports to agencies cannot be accomplished without computer systems. Analyses cannot be made, recorded, internally transmitted, organized and put into proper report format without use of computers and electronic manipulation. Reports are created from compilation of computerized data, proofed and stored in electronic media. The proposal gives an impression that electronic records should not exist without official sanction from EPA which is to be based on a system yet to be developed. This puts current recordkeeping and electronically stored information in an uncertain status. Those who wish to continue to use existing systems are left in a quandary. It is difficult to see what the status of currently stored records will be under this proposal.

3. State data receiving systems

The proposal has little to say about the requirements for state data receiving systems other than such systems will need to have EPA approval. It is very difficult from the proposed rule to determine the handling of such approvals and what the costs will be to states or to regulated entities dealing with the states that get program approval. There is simply not enough information available, particularly since EPA is not addressing paper to electronic record conversions. EPA does not state how current paper and electronic records are to be handled. Records in a state may very well affect multiple data systems across several state agencies. For instance the Department of Environment and Conservation may have primary responsibility for an environmental reporting system, but records may well involve other agencies such as Health, Agriculture, and Transportation. This level of coordination would be a greater effort than a more modest approach dealing with a subset of records within a single state agency. It is difficult to address comments until better information is available.

4. Conversion of paper records

EPA's rule does not address conversion of paper records to electronic formats. There are few electronic recordkeeping systems that will not involve moving substantial amounts of historic paper into an electronic system, if for no other reason than to simply make those records available at a workstation. Computer search and find capabilities offer so many advantages in accessibility that electronic systems are to be preferred, especially as electronic storage costs drop below storage costs for paper records. It is useful to address a move to a paperless recordkeeping system (or, more likely a combined paper and paperless system). Existing recordkeeping systems will often include both paper and electronic records. Some electronic document storage is already being done. It is important for EPA to regulate recordkeeping systems in a way that addresses how the paper and electronic archiving will be meshed. There needs to be a

consistency of regulatory approach.

EPA does not need to invent practices used for these paper to electronic conversions. EPA may get an acceptable result by making criteria that generally accepted industry practices be followed. The actual standards regarding image quality and handling should probably not be specified in EPA proposed rules except by reference to other standards as they develop. There are industry practices which can be of great benefit to development of a rule. Organizations such as Association for Information and Image Management (AIIM) and the Association of Records Managers and Administrators (ARMA) are good sources for coordination on records management and migration issues and standards.

While EPA is not authorizing conversion of paper records to electronic records, it is difficult to see where EPA would have authority to prohibit such conversions. Many recordkeeping requirements do not specify that records be kept ON PAPER. At the present, electronic conversion and storage options are about the same or slightly less than the cost for paper systems. The conversion costs will probably remain high, but electronic storage will go down and become significantly cheaper than paper storage. There will be increasing pressure to move to electronic record storage of paper documents with or without EPA sanction. By the time EPA gets the current proposed rule developed and in place, electronic information storage will be cheaper than keeping paper copies and conversion costs may improve as well. EPA needs to address this issue now. An alternative is for EPA to trust those doing conversions to do a responsible and effective job of it. In most cases, the records will be handled responsibly and well by professionals. As noted below, the document and record storage that handles paper conversions can be easily fitted into a single archive system that handles electronic documents and records.

Page 46164 of the proposal states, "Importantly, today's proposal will not authorize the conversion of existing paper documents to an electronic format for record-retention purposes because no mechanism currently exists that can be relied upon in all cases to preserve the forensic data in an existing paper document when it is converted to an electronic form." There is no discussion about the need for such forensic evidence, whether loss of this forensic evidence would have significant effect on how programs are run, how often such forensic evidence has been used by the agency in situations where a case could not have been developed based on evidence that would be available using an electronic archive system. There is no discussion of the potential to record marks, fingerprints, etc. by using different frequencies other than visible light in the scanning process (in some cases fingerprints can be scanned as well as the visible light text and graphics). Even where fingerprints may be lost by a conversion process, there are still many advantages such conversions to electronic media offer. There must be a balancing of the risks and costs. Jim Whitters (in Handling Risk in Electronic Reporting Programs, page 2, posted on the EPA website page for the rule proposal) advises, "In general, states only proceed with criminal prosecutions when they have overwhelming evidence of wrongdoing and feel that the risk of losing cases due to signature issues is small." The same may well be true for cases depending upon forensics of paper. There should be more investigation and study of this issue in the discussion.

Paper conversions cannot be dismissed when addressing recordkeeping because

almost all electronic recordkeeping systems will be connected to the historic paper records. Even in cases where paper records will be retained, they will need to be reflected in electronic systems to some extent. The ideal would be to have a system which handles both the historic records as well as the future records in a consistent way. As suggested below the use of a formatted report as the record to be stored will accomplish this. If EPA is addressing recordkeeping at this time, EPA should take a comprehensive approach. EPA should address conversion of paper records to electronic storage, interfaces for paper and electronic storage and current electronic record status.

5. Public notice of changes to CDX

In general, it would be acceptable to make public notice of changes to CDX as described in the rule. A more acceptable solution may be to establish electronic feedback systems for these changes. The system needs to be flexible enough to change with technology changes without going through rulemaking every time new technology develops or problems must be fixed. An alternative approach may be to use the codification to set up a "standards" group to make recommendations and a forum for stakeholders. With representation from the various stakeholders, the body may be better able to handle the job of setting standards than using federal code of regulations for notices.

6. Use of electronic signature method

It is questionable whether the electronic signature method is the only worthwhile method to be pursued. The rule states that it is intended to be technology neutral, but offers the electronic signature method as its only option, a technology-specific option. Electronic signature method as proposed puts an emphasis on electronics and is apparently favored by EPA. It would also be rather expensive. There need to be other authorization mechanisms other than public key encryption/decryption schemes. The reason for using PKI schemes is based on a desire that submittals must not be repudiated, must not be submitted by mistake and should be received error-free. However, the level of risk of falsification or repudiation is probably exaggerated and less stringent measures may still be useful.

The rule proposal requires third party registration mechanisms for PKI. Smart cards are already commonly used in Europe. These identify the sender via biometrics as well as carry information for authorizations. The proposed rule states the electronic signature will be part of a registration process. Page 46172 says, "This requires at least that the registrant provide evidence of identity which can be verified by information sources that are independent of this individual and the regulated entity with which he or she is associated." I wonder if companies would be allowed to issue "smart cards" to identify their own employees and grant power for authorizations where such companies have that ability or is EPA intending to require use of a third party?

The electronic signature is merely a means to the end. It assumes the authorizing agent is not identified by other means. It assumes that there are no other ways to have an authorizing agent signal their intent in submission. In many cases the submitter is someone with whom the agency has a continuing and long-standing relationship. The electronic method chosen here emphasizes an

approach almost solely reliant on electronics and not upon the people involved. There are multiple options for making an authorization some of which may involve people, access and place. There are many ways to make identification, and no doubt, there will shortly be other identification capabilities via electronic means. A reasonable level of proof is required. Enforcement cases are rarely developed on the basis of a single report or single signature. Most are based upon a preponderance of evidence. The regulated community, the regulators and third parties all recognize that human error plays a part in the process. A foolproof level of evidence may be too much to ask, too expensive and unnecessary. It is unclear that electronic signatures are the only methodology that should be acceptable. A great deal of detail is given to electronic signatures and no discussion is given for alternatives.

7. Goals of electronic signature and signature registration

The rule correctly states that the goal of electronic signatures should be identification of the sender and recording of the intent of the submitter in making a submittal. The certifications seem to be set up to meet other goals as well. The other goals attempted to be addressed by the convoluted system of certifications are not useful. The other goals, such as instructional/educational material, attempting to control the employer-employee relationships, etc. should not be squeezed into any certification scheme. There is some responsibility on the part of those using the certification and it should be part of the process without unnecessarily making the situation more complex.

The signature itself should not need extensive verbiage to establish the intent of the signature, identify the holder of the signature or prevent signature repudiation. If EPA wants to have a certification, it should stick to the details that are important. A shorter signature certification/registration statement may be as follows.

I understand and agree that I will be held as legally bound, obligated, or responsible by my use of my electronic signature as I would be using my hand-written signature, and that legal action can be taken against me based on my use of my electronic signature in submitting an electronic document to [specify the name of the receiving agency]. I understand that my electronic signature signifies my personal authorization and that I have a personal responsibility to maintain security and integrity for my electronic signature. Submittal of my signature by another should be understood as a forgery of my signature. If I become aware that my electronic signature is compromised, I will invalidate it, discontinue its use, and replace it with another, valid electronic signature.

For its part, the receiving system should inform the signatory "The signatory will not be held responsible for security lapses 1) on the part of the systems to which she/he submits data, 2) on the part of the transmission facilities for electronic transfers involving the signature, nor 3) on the part of those who register the electronic signature." This last is not a guarantee, but at least it acknowledges that responsibility for security involves more that just the signatory.

EPA also states that the registration/certification process is intended to

"ensure that the holder of an electronic signature understands how to properly use and protect the electronic signature." Based on these good intentions, it may be wise for EPA to explain what hand-written signatures mean. I personally believe most people know what a signature is and how it is used in business transactions. Educational drivel on what a signature is, what it means to a signatory, how it should be used, etc. is not appropriate and should not be squeezed into the verbiage thinly disguised as "certification." It takes up space and serves no real purpose. EPA should feel welcome to educate on issues of integrity, security, and the protection of privacy. It should not be part of certification and registration forms. It may be nice for EPA to inform people "If you no longer work for a company, you should not be certifying that company's information," but this is really a company's concern. When EPA is trying to control things to this level, it is overstepping the bounds of what it should be taking responsibility for. Similarly, the idea of a surrender certificate seems ludicrous. If I get fired or walk away from my employer, why would I sign a surrender certificate? If the only reason I sign is because EPA or my company threatens me, is such certification trustworthy? Responsible employees will justifiably see this kind of excess paperwork as an insult, and the paperwork probably will have no effect on the irresponsible or dishonest. Such certifications and repetitions serve no real purpose.

Page 46174 of the discussion seeks comment on whether codifying such a provision (providing additional certification or testimony that a specific electronic signature is legally binding) would provide a better method of ensuring the proper use and protection of signatures than the agreements, renewals and related certification statements that we are currently proposing. Unethical behavior is not thwarted by masses of verbiage. Beyond the recognition that an electronic signature is legally binding, no amount of additional certifications and signed statements are serving much purpose. One improvement would be for the intent of the signature to be included with the submittal document to which the electronic signature is attached. Thus, the "I hereby certify that to the best of my knowledge ..." statement should be part of the submittal. It is probably wiser to go with a simpler system than one with complex certifications. Many states will have laws that establish validity of electronic signatures within state borders. It may be wise to use existing law rather than rely upon special, federally-promulgated rules within the environmental context.

8. What is to be covered by certification of a report

It is worthwhile to note what is certified in much of the current reporting. A corporate official is responsible for summary reports. Backup information to the signed report is a responsibility of that official who sees that all reasonable quality control and data integrity measures are taken. A critique of record quality is one of the roles of inspection and evaluation by regulators. As an example, an NPDES monitoring report (DMR) is a summarized form with data for a month. It does not include the individual data points but reports information required for determination of permit compliance. There may be 30 or more data points for a reported pollutant parameter, but the submitted document may only have the maximum and average.

The signature of the responsible corporate official goes on the paper copy to carry an assurance that the information on permit compliance is true and

accurate information as well as to take responsibility for the information presented. In many cases, the truth and accuracy is not something that the signatory can personally verify and attest to. A manager's reliance on truth and accuracy in the report rests on the personnel and procedures that produce the report. In a few cases where reports are lengthy and complex, the signatory may not be physically able to check on the truth and accuracy of all information in a report that comes out each month. (A monthly submittal can run to more than a hundred pages of densely packed information.) The primary decision on what is 'good enough' for a manager to be able to certify with a high degree of confidence is left in the hands of responsible management who certifies the report.

The approach used in paper systems should not change for the electronic certification mechanisms. The certification should show 1) an intention to submit the report, 2) the fact that the information is believed to be true and accurate at time of submittal, and 3) the fact that a report received appears to be the same as the one sent. Certifications beyond this raise more problems than they solve. For instance, I have some concern raised by a certification that the signatory has reviewed ALL acknowledgments and copies of previous submissions. How is a signatory to even know that she has received all acknowledgments sent by the receiving system? Presumably, if someone is forging my signature, the forger will take steps to see that acknowledgments do not arrive at the correct destination/are hidden from view, etc. Given the possibility of nefarious activity, how would I know I have even received all, much less make certification of it. Also, as noted below, it could be a daunting, if not outright impossible, task to make reviews of ALL information in previous submittals. The signatory is often not personally involved in transcribing all data and verifying it. This is often done by others with certain quality controls in place. For me to make a personal review and certification for ALL data is quite simply not practical.

Page 46171 states, "A system that is used to receive electronic documents must be capable of reliably generating proof for use in private litigation, enforcement proceedings, and criminal proceedings in which the standard for conviction is proof beyond a reasonable doubt that the electronic document was actually submitted by the signatory and that the data it contains was not submitted in error." That a document was sent by the signatory is a valid concern to be addressed by the system. That the data was not sent in error is too difficult to establish with a computer system. Errors will occur where humans are involved. The important point is that the signatory realizes what the signature is attached to and authorizes it.

It is silly to go to an extreme level of effort to prevent deniability of erroneous reporting. The software requirements proposed seem such an extreme. A hundred-page submittal going under a single signature each month is not likely to get good personal review by a single signatory from a pragmatic, physical standpoint. In many cases, the signatory is taking responsibility and authorizing the submittal, but the validity of information is often delegated to others. It is not practical to require a signatory agree to the review all submittals for completeness/errors in on-screen format. The goal of getting good reports is not efficiently met by causing a user to scroll past massive amounts of information to ensure "the submitter reviews the data ... without

time constraint." From the standpoint of ergonomics, it is not possible to do this accurately. Time constraints are built into the reporting systems for EPA submittals. There is usually a deadline to be met. Analyses for the end of a month may take a week to get back. Then the data have to be compiled, put into proper format, proofed and submitted within the next week. Setting up screen after screen to be scrolled past is not useful to the regulated or the regulators. It is better to emphasize the final report created rather than some on-screen process standards that are not serving a pragmatic goal of reducing error.

Distinguishing deliberate falsification from erroneous reporting comes down to an evaluation of intent. Motive is important. Proof of intent cannot be any more easily established with a computerized system than in the paper system. This is a decision for a judge, board or jury. Computerized data review is not more likely to establish intent regardless of whether the time-constrained certification of error-free information is present or not. It may be that legal prosecutions are poorly handled and cases are lost. But judges and juries have to decide what is or is not responsible behavior based upon a preponderance of evidence. Juries do not need extra verbiage to render a decision where there is a preponderance of evidence. The value of causing signatories to page through large amounts of data on-screen prior to having an acceptable report is questionable in my mind.

9. Reliance should be on report documents, not the software interfaces and interactions

It will be difficult and unnecessary to track all the screen actions and maintain copies of all iterations of software specific to each submittal. All software screens and messages of the current software version need not be saved if the emphasis is put on the end product the user creates, reviews and intentionally sends as the report document. Raster image(s) of a report page(s) are easily stored and should be used rather than an attempt to use software screens. It is wise to require raster image files be preserved for certification pages, and for a final report format that can be reproduced on paper serve as the official "document." If the data must also be presented in a particular format besides the image file, such as for data uploads, that data file should be created at the time the certified report file is output as an image file.

An example of this is the PDF format mentioned above. The PDF format can contain the image of a report, as well as words and text strings stored separately that are searchable by the computer. Both are generated at the same time and contain the information. In a similar way, software should create an image file of the submittal report and a database-friendly format for importation into databases, word processors, etc. There is some small chance that an image file may differ from the data file because of some software problems. Software problems can and should be corrected where inconsistencies occur. However, the image file of the submitted report should be the controlling record for documentation purposes. It can be reviewed on-screen or be printed off and reviewed by human eyes on paper. It can have the necessary warnings and certifications contained within it.

Use of such an image file of the report would enable easy integration into electronic archive of other paper information since most paper to electronic conversions will be using a similar strategy. Reports that are the focus of certification with attendant warning messages should be sufficient for reporting. The user experience in creating his or her report should be immaterial. The user should be responsible for the certified report. A user will often not be directly responsible for the computer software and hardware operations.

A commonly used strategy for archiving in current electronic document systems may be followed. These would emphasize the final product of the submitter along with whatever warnings and certifications are necessary. The report, Records Management Storage Architecture Report submitted to EPA and dated October 1, 1999, (posted on the EPA web site for the proposed rule) suggests this strategy. Under section 4.5 Conversion Issues the report states

"While it is possible to store digital data in its native format (i.e., a WordPerfect 8 file, or a Freelance Graphics file) this creates problems with discontinued software, and possibly problems as newer versions of software are published. Historically, newer software versions have been backwards compatible. However, there are no guarantees this trend will continue indefinitely. This highlights the need for a common digital format for archival. This common digital format would actually be a digital "image" of the document. A recent study by the Department of Defense listed Tagged Image File Format (TIFF) and Portable Document Format (PDF) as the two most common image formats in use by the government today."

Emphasis on interaction with software is a bad strategy. The proposal suggests that besides requiring the signatory to page through what, in some cases, will be a mind-numbing experience of tens of screens, that all the software screens, warning messages, etc. should be saved. This would allow some judge and jury to experience the same miseries the software inflicts upon a user to make a report. But replication of the "user experience" cannot be guaranteed because software versions and hardware setups cannot be accurately replicated. There are too many variables to accurately replicate any particular user's experience. I have seen programs developed for 1024x768 screens that were exported to computers set up for 800x600 screen resolution. The result was that some "buttons" and choices were not available to the user and there was no way for the user in this case to even realize "part of the screen was missing." Many settings can have a potential effect. Even if all settings on similar computers are set the same, it will be impossible to replicate driver settings, memory status etc, to reliably replicate a user's experience. I may get a program to die on my computer with page fault errors, but I cannot reliably get my computer to do it at exactly the same point and in the same way each time. If the user has a Windows operating system crashes and presents the "Blue Screen Of Death" during data entry, should it be replicated so that a court to understand the user experience? It is unlikely that a BSOD will be created at the same point in a program, even on the same hardware and software. Putting emphasis on the software used to make reports is simply a terrible strategy. Data should be presented in a "report" format and it should not matter how that report was created. It should matter that the "report" be reviewed and sent by a certifying authority. It is not useful to document whatever computer miseries a

user goes through to organize information and create the report. What needs documentation is the report that is submitted and this should be presented to the user as a certifiable report. Emphasis should remain on the submitted report not on the software.

10. Exact copies, alteration of records/documents, changes of media.

On page 46171 and 46172 the document receiving system data goals are given and include: "that the document was not altered from the time it was sent to the time it was received" and "the system must reliably store and retrieve the document and associated metadata without alteration." It is probably best to state that the document received was the same as the document sent rather than stating that it will not be altered. A document in transit will be altered in that it will probably be broken into packets which may be sent and re-sent, may undergo compression, etc. The point to be made is that the received document is the same as the sent document. In fact, some alterations can occur. A similar concern is expressed below concerning the electronic recordkeeping system. If a record is moved from magnetic media to optical media is this an "alteration?" The important point is that the meaningful content not be altered. An alternative would be to give a definition of what EPA means by the term "altered." Alteration should not include the routine and regular processes involved in data management and storage.

11. General system security

The system security must include provisions for deletion of records. Not all records will be maintained in perpetuity. Further, some records will have to be modified/replaced/amended to correct errors in submissions.

The system obviously should not be corrupted or compromised, but it is likely to be found faulty at some point. It will be wise to have procedures developed and ready for implementation where systems do become corrupted. There will need to be disaster recovery, record replacement, etc. built into any system.

Similarly, when data is received that differs from what was sent or is in other ways invalid, the system must have established procedures for dealing with this situation.

12. Loss of Ability to Interpret Signatures With Passage of Time

It is more important that the archivist mark the submittal as a sealed document that will not be altered without change of content than that the electronic signature itself remain meaningful. It is important to store the electronic signature with the submitted document. However, due to passage of time, there is a valid concern that such signatures may not be interpreted in the future. For that reason, it is more important that receiving system indicate its recognition of the status of the submittal as part of the metadata for a submittal. If the submittal is judged invalid, that judgment should be attached to the metadata for the document. If the submittal is recognized as valid, the validity should be written in the permanent metadata associated with the record at the time the judgment is made. If the signature can no longer be read at some later time, at least the official status of the record as received or

reviewed is part of the documentation.

13. Revocation of an electronic signature

Page 46174 states that the receiving systems should revoke an electronic signature "whenever 1) there is any evidence the submitter has violated the registration agreement; 2) there is any evidence the electronic signature has been compromised; or 3) there is notification from an entity that the holder of an electronic signature previously authorized to represent that entity is no longer authorized to represent the entity." It should be noted that this stands in stark contrast to the bureaucracy set up to establish the signature in the first place. While there are identification/authentication measures in place to establish a signature, ANY evidence will apparently serve to revoke a signature. This implies no process, review or criteria set up for revocation. It almost seems to allow revoking an electronic signatures on little more than a personal whim. A system should not be set up such that I can make an anonymous phone call and disrupt another's submittals. This would not be a good thing. It is sensible that revocation be quick where signatures are compromised, but the system needs to have mechanisms developed for deciding when a revocation is or is not to be made based upon responsible and credible evidence. Systems should have follow-up, investigation and due process in these situations. The requirement should drop the word "any" and simply state that revocation will be made based on evidence. Criteria may be left to the specific receiving systems

14. Acknowledgments of submittals by receiving system

Acknowledgment of a submittal should be sent to the place designated by the sender. While it is good to send acknowledgment to some place other than the system with the same access control, this should remain a suggestion and not a requirement. Small operations may not have the luxury of multiple systems. Use of physical United States Postal Service address may be too slow a response time for some. The entity to make electronic submissions should be given the option of designating the place and the method of acknowledgment. Discussion for the CDX refers to automatic acknowledgment generated by the system. However, the important point seems to be that acknowledgment is made, not whether it is automatic. The proposed definition of "acknowledgment" does not indicate that the response must be an automated one.

15. Copy of Record

The copy of record should be created and available. My preference would be a simple image file of report pages be set as the standard for all copies of record. At any rate, the format of the copy of record should be established between the sender and receiving system before submissions are allowed. The copy of record should be in a format acceptable to the sender.

16. Transaction Record

In this age of Denial-of-Service attacks, it may be unwise to require receiving systems to accept and create a transaction record for every document sent to a receiving system. It may be wise to create transaction records for documents that are accepted as submittals. Breaks through a firewall, spurious contacts

and virus attacks should not require permanent record as "transactions." The person in charge of the system should have freedom to designate what is accepted as a record. The submitter should have a way to note a submittal was attempted at a certain time and date. If a receiving system is down from virus attack, hardware problems, etc., a mechanism needs to be in place to recognize that a submittal was attempted. There are various strategies that could be employed.

17. System Archives

As noted elsewhere, while the system acknowledgment, copy of record and transaction records will necessarily be part of the receiving system archives, records will also involve both the electronic recordkeeping and paper records used by the agency or submitting entity.

An image file that is preserved should have a certain required resolution to make sure all written parts are legible to the human eye when printed on paper. Other analog materials that are part of the record should also be preserved (voice recordings, photographs, etc.) in a way that allows the information to retain its meaning when retrieved from the archive and presented to the human eye, ear etc. The idea of preserving the record should not require the maximum resolution possible. Recording of analog information should merely be of such resolution as fits the purpose for which the data was collected.

Page 46176 states "In addition we are also proposing that the system must maintain records that show, for any given electronic submission not only what information was displayed to the user during the submission process - including the instructions, prompts, data labels, etc. captured in the copy of record - but also how this information was displayed, including the sequencing, functioning and overall appearance of these interface elements. The reason is that it may be difficult to interpret what some of the submission's data elements mean if we do not know the context within which they were provided - e.g., to what on-screen display or query a "yes" was responding. Depending on exactly how the signing process is implemented, at least some of this interface information may be captured within the scope of what is bound by the signature, e.g., if the signature is applied to the entire content of the screens that are reviewed by the signatory during the signature/certification scenario. To whatever extent this occurs, the archiving of the "copy of record" would contribute to this archiving of the interface."

This is an unacceptable strategy. Retaining a copy of the software in the archive is not a problem, but it seems a strategy that will be wasteful, hard to track, and uncertain to be replicated with changes to computer systems after the passage of time. Getting copies of all iterations of computer versions and tracking them through time is a big task. Emphasis must remain on report DOCUMENTS and not be misplaced on the changes to systems that generate documents. This is best done with documents that are presented as finished reports which can be recorded as image files.

The fact that the contents of the record will not be altered should not apply to the necessary and unexceptional maintenance functions for record archives or for creating copies of records. Examples would be such things as error correction code (ECC) used to reduce disk errors that develop with time or compression

algorithms used in archiving that do not change contents. ECC algorithms are a routine for data copying and maintenance of data. Such activity should not count as "modification" of a record. However, it should be clear that the record contents must be maintained such that accurate, unaltered information will be retained for the records.

18. Definitions

This definition of "electronic document", "communicate", "receive", "submit" and "electronic record" should also include awareness that records may be created or, for documents, the intent of the originator of the document to submit the document. Information passing back and forth between someone and a representative of an agency is not necessarily a document or record to be stored. The current definition is very broad and seems to allow almost any sort of information that either exists in digitized format or that can be converted into digitized format to become an "electronic record." This covers an extremely wide range of materials, a phone conversation, pictures, video, etc. There needs to be clear indication that "submitted" information in the document is officially being committed to the agency for consideration. Records should not be incidental telephone conversation that was not intended as a part of a document submission or record. For example, information gathered from a permittee should not be set up as a "record" without consent of a permittee. Both sides of the transaction have to be aware of the status of the information conveyed. There may be phone conversations which are official communication to an agency and thus have status as a document. Caution may need to be exercised that casual phone conversation with an agency representative or other unintended materials not be seen as an official record. For submittals that have an electronic signature attached, this will not be a problem. Other information without a signature process needs to have some protections of privacy and of consent about what is to be valid communication in records.

The definition for "electronic document" should not have the exclusion shown in the proposed rule. The proposal intends that currently submitted information using diskettes, tape, etc. not be regulated by the proposed rule. While discussion of the electronics documents emphasizes transmission of a submittal to an agency, the proposed rule also must address electronic recordkeeping systems. Those same recordkeeping systems will store "documents" sent either through telecommunications as well as information transmitted on diskettes, etc. There will be no particular difference between the two groups of records for recordkeeping systems other than the way they were transmitted to the agency. Putting an exclusion within this definition creates an artificial distinction that will end up costing money for little purpose. Electronic recordkeeping will have to handle both and should handle them similarly. If the electronic information recordkeeping system apply only to electronically transmitted documents, where will the other electronic reporting be stored? The definition gets unnecessarily confusing by including an exclusion. Whatever the mode of transmission, metadata for the "document" should be maintained which will indicate where the information came from, where it was sent and how it was handled.

The term "electronic document" should apply to all submitted documentation in electronic formats. Rather than shoehorn an exclusion into the definition, a

flat statement should be made that "electronic documents" submitted on diskette, etc. do not have to follow the same criteria as "electronic documents" transmitted to an agency via telecommunications. Another approach would be to substitute a more specific term, such as "Electronically transmitted document" that would be defined as "material of official business submitted to an agency or a third party for consideration in the form of an electronic record and communicated via a telecommunications network." If this definition were to be used, it would probably be useful to define an "electronically stored document" for recordkeeping purposes which could include all submitted documents regardless of how transmitted to an agency.

Definition of "electronic record" should have the term "meaningful information" substituted for the word "information." Some information created by computer may be in error, may be corrupted, etc. and should not be considered as a record. Some information is not relevant and should not be archived. Material that is to be maintained and recorded must be meaningful - not merely something created by a computer. It is conceivable in our age of Denial of Service attacks, computer viruses, worms, etc. that information may be created and transmitted by computer that will have no valid meaning. Such garbage should never be given the status of a "record" in the library/archive which should deal with meaningful information.

The definition, "electronic record-retention system," uses the term "exact electronic copies." This term should be changed or given better explanation. "Exact" seems to imply that a bit on the media cannot be corrected during copying. This would have unfortunate consequences for document maintenance on digital media. The intent of the rule is that the content of the records and documents should be copied accurately. Accuracy means that the standard code that routinely corrects disk errors should be allowed to correct corrupted disk information and thus, to restore the contents of the record and document to its original state. It is the method by which information is protected in electronic storage. This will not be an "exact" copy in that as disk errors are rewritten they are corrected. Without allowing error correction algorithms, electronic archives lose information and this defeats the purpose of recordkeeping. ECC is necessary, beneficial and should be allowed in record storage systems. The intent should emphasize preservation of record contents.

Thank you for allowing me the opportunity to comment.

Larry Bunting, TN Division of Water Pollution Control
401 Church St, 6th floor Annex
Nashville, TN 37243
voice: 615-532-0665
Email: Lawrence.Bunting@state.tn.us

Lawrence Bunting
<Lawrence.Bunting@state.tn.us>

02/27/02 03:33 PM

To: docket.oeca@epamail.epa.gov
cc:
Subject: docket #EC-2000-007 comments on CROMERR

Attached is a file (LarryBuntingComment.txt) in ASCII text format. This is my comment on the EPA's proposed electronic records rule, docket #EC-2000-007.

Larry Bunting, TN Water Pollution Control
Voice: 615-532-0665
Fax: 615-532-0686
Email: Lawrence.Bunting@state.tn.us

LarryBuntingComment.